PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-146788
(43)Date of publication of application : 06.06.1995

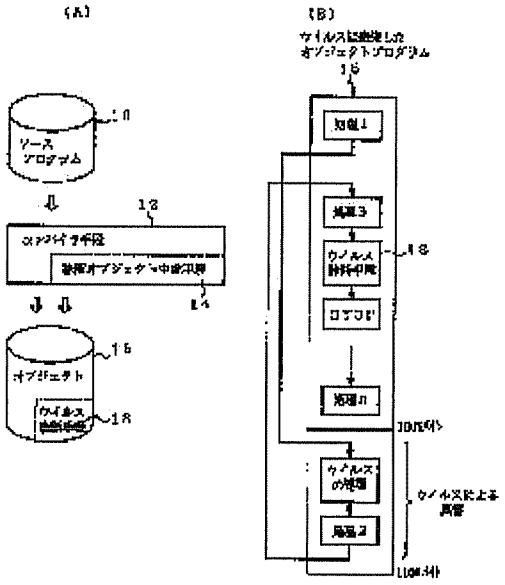
(51)Int.Cl. G06F 9/06
G06F 9/06
G06F 9/06
G06F 9/445
G06F 9/45
G06F 11/34

(21)Application number : 05-291658
(22)Date of filing : 22.11.1993

(71)Applicant : FUJITSU LTD
(72)Inventor : YAMAMOTO GOJI

(54) SYSTEM AND METHOD FOR PREPARING VIRUS DIAGNOSTIC MECHANISM AND VIRUS DIAGNOSTIC MECHANISM AND DIAGNOSTIC METHOD

(57)Abstract:
PURPOSE: To make it possible to diagnose virus infection by the OS of a computer or an object program itself to be executed as a program.
CONSTITUTION: When a source program 10 is converted into the object program 16 which is possible to be executed by a computer by a compile means 12, a virus diagnostic means 18 is generated in the object program 16 by a diagnosis object generation means 14 provided as one function of the compile means 12. The diagnostic means 18 performs the verification of the program size, the verification of a check sum, the verification of revision information on a preparation date month and year, etc., the verification of a disk address, the verification of an object program itself and the verification of the object program itself for which compression and restoration are utilized.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－146788

(43)公開日　平成７年(1995)６月６日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　9/06	５５０　Ｚ	9367－5B			
	４１０　Ｐ	9367－5B			
	５３０　Ａ	9367－5B			
		9367－5B	Ｇ０６Ｆ　9/06	４２０　Ｓ	
		9292－5B	9/44	３２２　Ｚ	

審査請求　未請求　請求項の数36　ＯＬ　（全 17 頁）　最終頁に続く

(21)出願番号　特願平5－291658

(22)出願日　平成５年(1993)11月22日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　山本　剛司
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

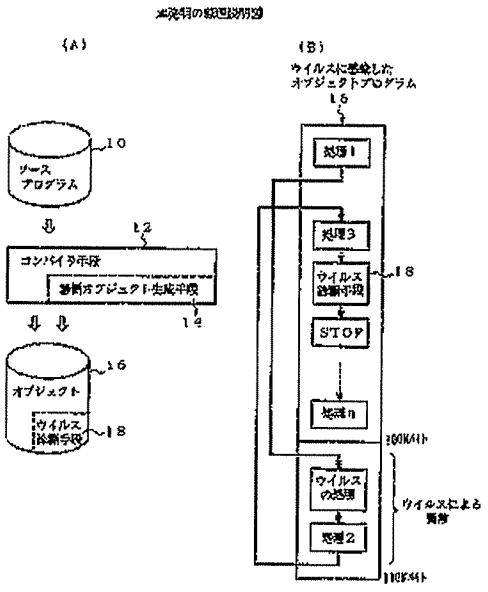
(74)代理人　弁理士　竹内　進　（外１名）

(54)【発明の名称】　ウイルス診断機構の作成システムと作成方法並びにウイルス診断機構と診断方法

(57)【要約】

【目的】計算機のＯＳ又はプログラムとして実行されるオブジェクトプログラム自身でウイルス感染を診断できるようする。

【構成】コンパイル手段１２でソースプログラム１０を計算機で実行可能なオブジェクトプログラム１６に変換する際に、コンパイラ手段１２の１つの機能として設けられた診断オブジェクト生成手段１４によって、オブジェクトプログラム１６の中にウイルス診断手段１８を生成する。ウイルス診断手段１８は、プログラムサイズの検証、チェックサムの検証、作成年月日等のレビジョン情報の検証、ディスクアドレスの検証、オブジェクトプログラム自身の検証、圧縮復元を利用したオブジェクトプログラム自身の検証などを行う。



1

【特許請求の範囲】

【請求項１】ソースプログラム（１０）を計算機で実行可能なオブジェクトプログラム（１６）に変換するコンパイラ手段（１２）と、

前記コンパイラ手段（１２）に設けられ、前記オブジェクトプログラム（１６）の中にウイルス診断手段（１８）を生成する診断オブジェクト生成手段（１４）と、を備えたことを特徴とするウイルス診断機構の作成システム。

【請求項２】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルサイズを格納したオリジナルサイズ格納手段と、

前記計算機のオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラム（１６）のサイズを検出する実行サイズ検出手段と、

前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

【請求項３】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのチェックサムを格納したオリジナルチェックサム格納手段と、

前記計算機のオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出手段と、

前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

【請求項４】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出手段と、

前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

2

【請求項５】請求項４記載のウイルス診断機構の作成システムに於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも１つを用いたことを特徴するウイルス診断機構の作成システム。

【請求項６】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）の格納先を示すディスクアドレスを格納したディスクアドレス格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出手段と、

前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

【請求項７】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）をオリジナルとしてそのまま格納したオリジナル・オブジェクト格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込手段と、

前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。

【請求項８】請求項１記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルを圧縮して格納した圧縮オブジェクト格納手段と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込手段と、

前記圧縮オブジェクト格納手段の圧縮オブジェクトプロ

グラムを伸長して元に戻す復元手段と、
前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構の作成システム。
【請求項９】請求項２，３，４，５，６又は７記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成手段（１４）により生成された前記ウイルス診断手段（１８）は、更に、前記オブジェクトプログラム（１６）の実行によるプログラム自身の書き替えを禁止する更新禁止手段を付加したことを特徴とするウイルス診断機構の作成システム。
【請求項１０】ソースプログラム（１０）を計算機で実行可能なオブジェクトプログラム（１６）に変換するコンパイル過程と、
前記コンパイル過程において、前記オブジェクトプログラム（１６）の中にウイルス診断手段（１８）を生成する診断オブジェクト生成過程と、を備えたことを特徴とするウイルス診断機構の作成方法。
【請求項１１】請求項１０記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイル過程で変換された前記オブジェクトプログラム（１６）のオリジナルサイズを格納するオリジナルサイズ格納過程と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを検出する実行サイズ検出過程と、
前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１２】請求項１０記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのチェックサムを格納したオリジナルチェックサム格納過程と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出過程と、
前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１３】請求項１０記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイラ過程で変換された前記オブジェクトプログラム（１６）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納過程と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出過程と、
前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１４】請求項１３記載のウイルス診断機構の作成方法に於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも１つを用いたことを特徴するウイルス診断機構の作成方法。
【請求項１５】請求項１０記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイル過程で変換された前記オブジェクトプログラム（１６）の格納先を示すディスクアドレスを格納したディスクアドレス格納過程と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出過程と、
前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１６】請求項１０記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルとしてそのまま格納したオリジナル・オブジェクト格納過程と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込過程と、
前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１７】請求項１０記載のウイルス診断機構の作成システムに於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、
前記コンパイル過程で変換された前記オブジェクトプログラム（１６）のオリジナルを圧縮して格納する圧縮オブジェクト格納過程と、
前記計算機でオペレーティングシステムまたはプログラ

ムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込過程と、
前記圧縮オブジェクト格納過程の圧縮オブジェクトプログラムを伸長して元に戻す復元過程と、
前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断機構の作成方法。
【請求項１８】請求項１１、１２、１３、１４、１５、１６又は１７記載のウイルス診断機構の作成方法に於いて、前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は、更に、前記オブジェクトプログラム（１６）の実行によるプログラム自身の書き替えを禁止する更新禁止過程を備えたことを特徴とするウイルス診断機構の作成方法。
【請求項１９】計算機で実行可能な形式に変換されたオブジェクトプログラム（１６）の中に、前記計算機のオペレーティングシステム又はプログラムの一部として実行されるウイルス診断手段（１８）を設けたことを特徴とするウイルス診断機構。
【請求項２０】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルサイズを格納したオリジナルサイズ格納手段と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを検出する実行サイズ検出手段と、
前記オリジナルサイズと前記実行時のサイズとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するサイズ判断手段と、を設けたことを特徴とするウイルス診断機構。
【請求項２１】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのチェックサムを格納したオリジナルチェックサム格納手段と、前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出手段と、
前記オリジナルチェックサムと前記実行時のチェックサムとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するチェックサム判断手段と、を設けたことを特徴とするウイルス診断機構。
【請求項２２】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納手段と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出手段と、
前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するレビジョン判断手段と、を設けたことを特徴とするウイルス診断機構。
【請求項２３】請求項２２記載のウイルス診断機構に於いて、前記レビジョン情報として、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも１つを用いたことを特徴するウイルス診断機構。
【請求項２４】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）の格納先を示すディスクアドレスを格納したディスクアドレス格納手段と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出手段と、
前記オリジナルのディスクアドレスと前記実行時のディスクアドレスとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較手段と、を設けたことを特徴とするウイルス診断機構。
【請求項２５】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルとしてそのまま格納したオリジナル・オブジェクト格納手段と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込手段と、
前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたことを特徴とするウイルス診断機構。
【請求項２６】請求項１９記載のウイルス診断機構に於いて、前記ウイルス診断手段（１８）は、
前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルを圧縮して格納した圧縮オブジェクト格納手段と、
前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込手段と、
前記圧縮オブジェクト格納手段の圧縮オブジェクトプログラムを伸長して元に戻す復元手段と、
前記復元オブジェクトと前記実行オブジェクトとを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するオブジェクト比較手段と、を設けたこ

とを特徴とするウイルス診断機構。

【請求項２７】請求項２０，２１，２２，２３，２４，２５又は２６記載のウイルス診断機構に於いて，前記ウイルス診断手段（１８）は，更に、前記オブジェクトプログラム（１６）の実行によるプログラム自身の書き替えを禁止する更新禁止手段を付加したことを特徴とするウイルス診断機構。

【請求項２８】計算機で実行可能な形式に変換されたオブジェクトプログラム（１６）の処理過程の中に，前記計算機のオペレーティングシステム又はプログラムの一部として実行されるウイルス診断過程を設けたことを特徴とするウイルス診断方法。

【請求項２９】請求項２８記載のウイルス診断方法に於いて，前記ウイルス診断過程は，

前記コンパイル過程で変換された前記オブジェクトプログラム（１６）のオリジナルサイズを格納するオリジナルサイズ格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのサイズを検出する実行サイズ検出過程と，

前記オリジナルサイズと前記実行時のサイズとを比較し，両者が一致した場合は処理を続行し，不一致の場合は処理を中断するサイズ判断過程と，を設けたことを特徴とするウイルス診断方法。

【請求項３０】請求項２８記載のウイルス診断方法に於いて，前記ウイルス診断過程は，

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルのチェックサムを格納したオリジナルチェックサム格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのチェックサムを検出するチェックサム検出過程と，

前記オリジナルチェックサムと前記実行時のチェックサムとを比較し，両者が一致した場合は処理を続行し，不一致の場合は処理を中断するチェックサム判断過程と、を設けたことを特徴とするウイルス診断方法。

【請求項３１】請求項２８記載のウイルス診断方法に於いて，前記ウイルス診断過程は，

前記コンパイラ過程で変換された前記オブジェクトプログラム（１６）のオリジナルのレビジョン情報を格納したオリジナル・レビジョン格納過程と，

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのレビジョン情報を検出するレビジョン検出過程と，

前記オリジナル・レビジョン情報と前記実行時のレビジョン情報とを比較し，両者が一致した場合は処理を続行し，不一致の場合は処理を中断するレビジョン判断過程と，を設けたことを特徴とするウイルス診断機構の作成方法。

【請求項３２】請求項３１記載のウイルス診断機構の作成方法に於いて，前記レビジョン情報として、更新を含む作成年月日，更新を含む作成時刻，作成者名，プログラム名，バージョン番号の少なくとも１つを用いたことを特徴するウイルス診断機構の作成方法。

【請求項３３】請求項２８記載のウイルス診断方法に於いて，前記ウイルス診断過程は，

前記コンパイル過程で変換された前記オブジェクトプログラム（１６）の格納先を示すディスクアドレスを格納したディスクアドレス格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムのディスクアドレスを検出するディスクアドレス検出過程と，

前記オリジナルのディスクアドレスと前記実行時のディスクアドレス情報とを比較し、両者が一致した場合は処理を続行し、不一致の場合は処理を中断するディスクアドレス比較過程と、を設けたことを特徴とするウイルス診断方法。

【請求項３４】請求項２８記載のウイルス診断機構の作成方法に於いて，前記診断オブジェクト生成過程で生成された前記ウイルス診断手段（１８）は，

前記コンパイラ手段（１２）で変換された前記オブジェクトプログラム（１６）のオリジナルとしてそのまま格納したオリジナル・オブジェクト格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込過程と，

前記オリジナル・オブジェクトと前記実行オブジェクトとを比較し，両者が一致した場合は処理を続行し，不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断方法。

【請求項３５】請求項２８記載のウイルス診断装置に於いて，前記ウイルス診断過程は，

前記コンパイル過程で変換された前記オブジェクトプログラム（１６）のオリジナルを圧縮して格納する圧縮オブジェクト格納過程と、

前記計算機でオペレーティングシステムまたはプログラムとしてロードされた前記オブジェクトプログラムを読込む実行オブジェクト読込過程と，

前記圧縮オブジェクト格納過程の圧縮オブジェクトプログラムを伸長して元に戻す復元過程と，

前記復元オブジェクトと前記実行オブジェクトとを比較し，両者が一致した場合は処理を続行し，不一致の場合は処理を中断するオブジェクト比較過程と、を設けたことを特徴とするウイルス診断方法。

【請求項３６】請求項２８，２９，３０，３１，３２，３３，３４又は３５記載のウイルス診断方法に於いて，前記ウイルス診断過程は，更に、前記オブジェクトプログラム（１６）の実行によるプログラム自身の書き替えを禁止する更新禁止過程を備えたことを特徴とするウイ

ルス診断方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータウイルスの感染を予防するためウイルス診断機構の作成システムと作成方法並びにウイルス診断機構と診断方法に関し、特に、ワクチンが侵入した際に抗体として機能するウイルス診断機構の作成システムと作成方法並びにウイルス診断機構と診断方法に関する。

【０００２】

【従来の技術】近年のコンピュータシステムにあっては、コンピュータウイルスの発生に伴い、ウイルスに感染しない機能が要求されている。従来、外部から侵入したコンピュータウイルスの感染によりファイル破壊などの異常が起きた場合には、コンピュータウイルスの機能を無効化させるコンピュータワクチンなどを開発して提供することで、ウイルス感染を防止するようにしている。

【０００３】

【発明が解決しようとする課題】しかしながら、従来のコンピュータワクチンを用いたウイルスの感染防止にあっては、新型のウイルスが発生すると、ワクチンの開発にある程度の時間がかかるため、その間にウイルスに感染する恐れがあった。またウイルスに感染していても、ファイルが１つ消える程度の被害に気付くことはほとんどなく、ウイルス感染に気付くまでにファイル破壊などの被害が拡大してしまう問題があった。

【０００４】本発明の目的は、コンパイラによるオブジェクトプログラムへの翻訳段階でウイルス診断機構を自動的に生成し、ＯＳ又はプログラムとして実行されるオブジェクトプログラム自身でウイルス感染を診断できるようにしたウイルス診断機構の作成方法と装置並びにウイルス診断機構と診断方法を提供する。

【０００５】

【課題を解決するための手段】第１図は、本発明によるウイルス診断機構の作成システムを例にとった原理説明図である。本発明のウイルス診断機構の作成システムは、コンパイル手段１２とその中に設けた診断オブジェクト生成手段１４で構成される。コンパイル手段１２は、ソースプログラム１０を任意の計算機で実行可能なオブジェクトプログラム１６に変換する。

【０００６】診断オブジェクト生成手段１４は、コンパイラ手段１２の１つの機能として設けられ、オブジェクトプログラム１６の中にウイルス診断手段１８を生成する。診断オブジェクト生成手段１４により生成されるウイルス診断手段１８は、

①プログラムサイズの検証

②チェックサムの検証

③作成年月日等のレビジョン情報（改訂情報）の検証

④ディスクアドレスの検証

⑤オブジェクトプログラム自身の検証

⑥圧縮復元を利用したオブジェクトプログラム自身の検証

のいずれかの機能を実現する。

【０００７】［プログラムサイズの検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６のオリジナルサイズを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラム１６の実行サイズを検出してオリジナルサイズと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【０００８】［チェックサムの検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６のオリジナルのチェックサムを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのチェックサムを検出してオリジナルチェックサムと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【０００９】［レビジョン情報（改訂情報）の検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６のオリジナルのレビジョン情報を格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのレビジョン情報を検出してオリジナル・レビジョン情報と比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルス感染と判断して処理を中断する。

【００１０】ここで、レビジョン情報としては、更新を含む作成年月日、更新を含む作成時刻、作成者名、プログラム名、バージョン番号の少なくとも１つを用いる。

［ディスクアドレスの検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６の格納先を示すディスクアドレスを格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムのディスクアドレスを検出し、オリジナルのディスクアドレスと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルスに感染したと判断して処理を中断する。

［オブジェクトプログラム自身の検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６のオリジナルとしてそのまま格納しておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行された前記オブジェクトプログラムを読込んでオリジナル・オブジェクトと比較し、両者が一致した場合は処理を続行し、不一致の場合はウイルスに感染したと判断して処理を中断する。

【００１１】［圧縮復元を利用したオブジェクトプログラム自身の検証］コンパイラ手段１２で変換されたオブジェクトプログラム１６のオリジナルを圧縮して格納し

ておく。計算機でオペレーティングシステムまたはプログラムとしてロードして実行されたオブジェクトプログラムを読込み，同時に圧縮オブジェクトプログラムを伸長して元に戻す，そして復元オブジェクトと実行オブジェクトとを比較し，両者が一致した場合は処理を続行し，不一致の場合はウイスルに感染したと判断して処理を中断する。

【００１２】更に，オブジェクトプログラム１６の実行によるプログラム自身の書き替えを禁止する更新禁止手段を，ワクチンとしてコンパイルの段階で付加するようにしてもよい。さらに本発明は，コンパイラ手段１２の診断オブジェクト生成手段１４で生成されたウイルス診断機構１８，すなわちワクチン診断オブジェクトそのものを対象とする。

【００１３】

【作用】本発明によれば，コンパイラを用いてソースプログラムからオブジェクトプログラムに変換するオブジェクト生成時に，オブジェクト生成時にしか判らない情報としてのウイルス診断機構を生成してオブジェクトに埋め込んでいる。このため，計算機のオペレーティングシステムまたはプログラムとしての実行で，ウイルスによってオブジェクトが書き換えられた場合，オブジェクト自身がもつウイルス診断機構によって書き換えられたことをオブジェクトが認識できる。

【００１４】従って，オブジェクトがウイルスに感染した可能性があると判断した場合には，実行を中断し，ウイルスの被害を最小限に食い止めることが可能となる。

【００１５】

【実施例】図２は本発明によるウイルス診断機構を埋め込んだオブジェクトプログラムの作成に使用されるコンパイラマシンのハードウェア構成を示している。図２において，主記憶装置２００にはオペレーティングシステム（ＯＳ）が格納され，電源投入時にコンパイラを実現するプログラムが展開される。主記憶装置２００に対しては主記憶制御装置２０２が設けられる。主記憶制御装置２０２にはＣＰＵ２０４およびチャネルプロセッサ２０８が設けられる。

【００１６】ＣＰＵ２０４は主記憶装置２００に転換されたコンパイラプログラムに従って，ソースプログラムを計算機で実行可能なアッセンブラ語や機械語で表現されたオブジェクトプログラム（目的プログラム）に変換するコンパイルを行う。チャネルプロセッサ２０６のチャネル装置２０８には，チャネルバス２１０を介して磁気ディスクユニットなどを用いたファイル装置２２０，２３０，２５０，２６０が接続される。

【００１７】ファイル装置２２０にはコンパイルを行うソースプログラム１０が格納されている。ファイル装置２３０にはコンパイルの処理過程ごとに生成される中間ファイル２４０が格納されている。ファイル装置２５０にはコンパイルが済んだウイルス診断機構付きのオブジェクトプログラム１６が格納されている。更にファイル装置２６０にはコンパイルの処理過程で生成されるシンボルテーブル２７０が格納されている。

【００１８】勿論，チャネルプロセッサ２０６の他のチャネル装置には図示しないＣＲＴ，プリンタ，キーボードなどの他の入出力機器が接続される。図３は本発明によるウイルス診断機構付きのオブジェクトプログラムの生成機能の概略を示す。図３において，ソースプログラム１０はＣＯＢＯＬ，ＦＯＲＴＲＡＮなどの適宜のプログラム言語を使用して作成され，ファイル装置によるファイル情報として適用される。

【００１９】コンパイラ部１２はソースプログラム１０を入力し，対象となる計算機で実行可能なアッセンブラ語や機械語で表現されたオブジェクトプログラムへの変換処理を行い，ファイル情報としてオブジェクトプログラム１６を出力する。本発明にあっては，コンパイラ部１２の中に診断オブジェクト生成部１４が新たに設けられている。診断オブジェクト生成部１４はコンパイラ部１２でソースプログラム１０のオブジェクトプログラム１６への変換処理の際に，オブジェクトプログラム１６の中にウイルス診断機構１８を自動的に生成する。

【００２０】このコンパイラ部１２に設けた診断オブジェクト生成部１４によるウイルス診断機構１８の生成機能はソースプログラム１０に依存しておらず，ソースプログラム１０の内容の如何に関わらず，コンパイラ部１２を通すことで自動的にオブジェクトプログラム１６の中に埋め込まれることになる。従って，ソースプログラム１０の作成段階では本発明のウイルス診断機構１８を全く意識する必要はない。

【００２１】図４は図３の診断オブジェクト生成部１４を備えたコンパイラ部１２の機能構成を示した説明図である。このコンパイラとしての機能は，図２のＣＰＵ２０４によるプログラムの実行の形で実現される。図４において，コンパイラは語彙解析処理部２６，構文解析処理部３０，中間コード生成部３４，コード最適化部３８，コード生成部４４および診断オブジェクト生成部１４で構成される。

【００２２】語彙解析部２６にはソースプログラム１０が入力される。語彙解析処理部２６，構文解析処理部３０，中間コード生成部３４およびコード最適化部３８にあっては，中間ファイル２８，３２，３６，４２の各々が生成される。語彙解析処理部２６はＣＯＢＯＬやＦＯＲＴＲＡＮなどの所定のプログラミング言語で書かれたソースプログラム１０を入力し，プログラム言語の語彙を解析する。即ち，プログラミング言語で書かれたソースプログラム１０をトークンと呼ばれる単位ごとに区切り，その単語の正当性をチェックする。

【００２３】このトークンの代表例はキーワード，演算子，変数名，定数，区切り記号などがある。語彙解析部２６は全てのソースプログラム１０の語彙の正当性をチ

ェックした後で、トークンの集合でなる中間ファイル２８を出力し、次の語義解析処理部３０に引き渡す。

【００２４】構文解析処理部３０は語義解析処理部２６で生成された中間ファイル２８を入力し、ソースプログラム１０が使用されているプログラミング言語の文法規則に合致しているか否かチェックする。文法規則に合致していればソースプログラム１０を実行する手順を決め、同様に中間ファイル３２として出力する。この構文解析処理部３０による構文解析は、一般的には２つの機能を備えている。１つの機能はソースプログラム２６上の各トークンが文法的に正しい位置にあるか否かのチェックである。

【００２５】２つ目の機能はソースプログラム１０上の全トークンの存在意味を解析した後にこれらの実行手順を決め、その手続きをトークンの流れやグループ化として表現することである。一般には各トークンの実行順序の分析結果を表現するのに木構造（パースツリー）が使用される。中間コード生成部３４は構文解析処理部３０で作成された中間ファイル３２の木構造（パースツリー）を入力し、コンパイラがもっている固有の中間コードに変換し、中間ファイル３６を出力する。代表的な中間コードとしては３オペランド方式が知られている。

【００２６】コード最適化部３８は中間コード生成部３４に得られた中間ファイル３６の中間コードを入力し、ターゲットとなる計算機上で最も少ない容量で且つ最も早い速度で実行可能な中間言語に変換し、中間ファイル４２を出力する。一般的な最適化の手法としては、ローカルな最適化とループの最適化がある。ローカルな最適化とは余分な命令を減らすことである。またループの最適化とはループを毎回実行するごとに同じ値を示す式があるような場合は、これを無条件にループの外に追い出して最初の１回だけを実行するような方法である。

【００２７】コード生成部４４はコード最適化が済んだ中間ファイル４２の中間コードまたは中間言語をコード生成部４４に入力し、ターゲットとなる計算機の命令セットに変換する。これに加えて本発明にあっては、更に診断オブジェクト生成部１４を設けており、コード生成部４４より最終的な変換結果として得られたターゲットとなる計算機の命令セットの中に、更にウイルス診断機構１８を構成する命令セットを加える。

【００２８】このため、診断オブジェクト生成部１４により加えられるウイルス診断機構１８は、ターゲット計算機の命令セットでなるアッセンブラ語あるいは機械語で記述された状態で準備されている。勿論、ソースプログラムに用いたプログラミング言語やコンパイラにおける中間言語で表現されたウイルス診断機構を準備し、対応するコンパイラ過程の段階で変換プログラムの中に埋め込むようにしてもよい。

【００２９】診断オブジェクト生成部１４によるオブジェクトプログラムの中へのウイルス診断機構１８の埋込みが済むと、ファイル情報としてオブジェクトプログラム１６が出力される。このようにコンパイラでソースプログラム１０から変換されたウイルス診断機構１８を埋め込んだオブジェクトプログラム１６は、フロッピーディスク，磁気テープなどの媒体、あるいはオンラインにより対象計算機のＲＯＭやディスクユニットにプログラムファイルとして提供されることになる。

【００３０】図５は本発明によりソースプログラムの中に埋め込まれたウイルス診断機構１８の第１実施例を示した機能ブロック図である。図５において、第１実施例のウイルス診断機構１８はプログラムサイズ検出部２０、サイズ判断部２２およびオリジナルサイズ格納部２４で構成される。オリジナルサイズ格納部２４には図３、図４に示したように、コンパイラ部１２でオブジェクトプログラム１６を作成した際のプログラムサイズ、例えばバイト数が、診断オブジェクト生成部１４によるウイルス診断機構１８の生成時にセットされている。

【００３１】プログラムサイズ検出部２０は、このウイルス診断機構１８を備えたソースプログラムが計算機上のＯＳあるいはプログラムとして実行された段階で、プログラムがウイルス診断機構１８の処理に進む際の起動入力を受け、ウイルス診断機構１８が埋め込まれているオブジェクトプログラムのプログラムサイズが何バイトかを検出する。

【００３２】サイズ判断部２２はプログラムサイズ検出部２０より実行プログラムサイズが得られると、オリジナルサイズ格納部２４のオリジナルサイズと比較する。実行プログラムサイズがオリジナルサイズに一致していれば、ウイルス感染によるプログラム破壊がないことから続行出力を生じ、オブジェクトプログラムの中のウイルス診断機構１８の埋込み一致に続く次のプログラム処理にリターンする。

【００３３】これに対し、実行プログラムサイズがオリジナルサイズに一致しなかった場合には、ウイルス感染により異常な処理が加わってオブジェクトプログラムのプログラムサイズが変化していることが判る。この場合にはウイルス感染したものと判断し、中断出力を生じ、それ以降のオブジェクトプログラムの実行を抑止する。勿論、オブジェクトプログラムの中断に伴い、オペレータコンソールなどに対しウイルス感染による処理中断のメッセージ出力を行う。

【００３４】図６は図５に示したウイルス診断機構１８の第１実施例の処理動作を示している。図６において、オブジェクトプログラムの処理からウイルス診断機構の処理に移行すると、まずステップＳ１で、現在実行している自己のオブジェクトプログラムのサイズを検出する。

【００３５】続いてステップＳ２で、予め格納しているオリジナルサイズと比較して一致するか否か判断し、一致すれば再び正常なオブジェクトプログラムの処理に戻

る。一方、検出したプログラムサイズがオリジナルサイズに等しくなかった場合には、ウイルス感染によるプログラムサイズの変化と判断し、ステップＳ３で処理を中断する。

【００３６】図７はコンピュータウイルスの感染処理の一例を示している。図７のウイルスの感染処理にあっては、まずステップＳ１でＯＳまたはプログラムの最後にウイルス自身をコピーし、続いてステップＳ２でＯＳまたはプログラムからウイルスを呼び出すために破壊する命令を自分の最後にコピーする。そしてステップＳ３でＯＳまたはプログラムからウイルスを呼び出すように修正する。図８は図７の感染処理を行うウイルスに感染したオブジェクトプログラムについて、感染前と感染後のプログラム構造を示している。

【００３７】図８（Ａ）は感染前のオブジェクトプログラム４８を示し、オブジェクトプログラム４８は処理ブロック５０－１～５０－ｎに分けられた処理１～処理ｎを順番に実行する構造をもっている。このようなオブジェクトプログラム４８が図７のウイルスに感染すると、図８（Ｂ）の感染後のソースプログラム５２のようにプログラム構造が変化する。

【００３８】即ち、処理ブロック５０－１の処理１に続いてウイルスが自分自身をコピーしたウイルス処理ブロック５４を本来のソースプログラム４８の後ろに加えられ、続いてウイルスにより破壊された処理ブロック５２の処理２が加えられる。そして、再び元のソースプログラム４８の処理ブロック５３の処理３に戻るようなプログラム構造を作る。その結果、オリジナルのソースプログラム４８に対し、ウイルス感染による処理で増加領域６０がソースプログラム４８に加わるようになる。

【００３９】図９は図５に示したウイルス診断機構１８を埋め込んだ本発明のソースプログラムの感染前と感染後のプログラム構造を示している。まず図９（Ａ）は感染前の本発明によるソースプログラム４８を示しており、処理ブロック５０－３と５０－４で示される処理２と処理４の間にコンパイラの際に生成されたウイルス診断機構１８が埋め込まれている。

【００４０】このウイルス診断機構１８を埋め込んだオブジェクトプログラム４８のプログラムサイズは例えば１００Ｋバイトであり、これがオリジナルサイズとして図５に示したオリジナルサイズ格納部２４に予めセットされている。図９（Ａ）のオブジェクトプログラム４８がウイルスに感染すると、図９（Ｂ）に示すようにオブジェクトプログラム５６となる。このオブジェクトプログラムは、元のオブジェクトプログラム４８の最後にウイルス自身をコピーしたウイルス処理ブロック５４が追加され、続いてウイルスを呼び出すために破壊する命令として処理ブロック５０－３の処理２をセットする。そして、オブジェクトプログラム４８の処理ブロック５０－１の処理１からウイルスをコピーしたウイルス処理ブロック５４に至り、破壊対象となる処理ブロック５２－２の処理２から再びオブジェクトプログラム４８の処理ブロック５０－３の処理３に戻るプログラム構造を作り出す。

【００４１】このようなウイルスによる感染が処理ブロック５０－２の処理２について行われると、感染前１００Ｋバイトであったプログラムサイズが、感染により例えば１０Ｋバイトの増加領域６０が加わって１１０Ｋバイトのプログラムサイズに変化してしまう。このようなプログラムサイズの変化に対し、この例では処理ブロック５０－３の処理３に続いて図５に示したウイルス診断機構１８が設けられており、図６のフローチャートに従ったウイルス診断処理が実行される。

【００４２】この場合、プログラムサイズがオリジナルの１００Ｋバイトに対し１１０Ｋバイトと変化しているため、プログラムサイズの不一致からウイルスによる感染と判断され、ブロック５８に進んでオブジェクトプログラムの処理を中断することができる。従って、これ以上、オブジェクトプログラムを実行してウイルスによる感染が広がってしまうことを防止できる。また処理中断に伴ってオペレータコンソールにウイルス感染による処理中断のメッセージ出力をオブジェクトプログラムのプログラム名称や番号と共に行うことで、特定のプログラムやＯＳにウイルス感染が起きたことを通知することができる。

【００４３】図１０は本発明によるウイルス診断機構１８の第２実施例を示した機能ブロック図である。図１０において、第２実施例のウイルス診断機構１８はチェックサム検出部６２，チェックサム判断部６４およびオリジナルチェックサム格納部６６で構成される。

【００４４】コンパイラから出力されたソースプログラムは、ソースプログラムを格納するＲＯＭなどのメモリ装置における所定サイズのメモリブロックごとにチェックサムを求めていることから、この段階で得られたチェックサムをオリジナルチェックサムとしてオリジナルチェックサム格納部６６に格納している。図１０のウイルス診断機構１８を埋め込んだソースプログラムの実行により、前に位置する処理が終了して起動入力を受けると、チェックサム検出部６２でメモリブロック単位にチェックサムを検出し、チェックサム判断部６４で対応するブロックのオリジナルチェックサムと比較する。

【００４５】チェックサムが一致すれば続行出力を生じ、チェックサムが不一致であればウイルスによる感染と判断し、中断出力により処理を中断する。図１１は図１０のチェックサムを用いたウイルス診断機構１８の処理動作を示す。図１１において、まずステップＳ１でオブジェクトプログラムの先頭ブロックのチェックサムを検出し、ステップＳ２でオリジナルのチェックサムに等しいか否かチェックする。

【００４６】等しければステップＳ３に進み、全ブロッ

クを終了していなければ次のブロックに進み、ステップＳ１のブロックのチェックサムの検出とステップＳ２のオリジナルチェックサムとの比較を全ブロック終了まで繰り返す。全ブロックについてチェックサムがオリジナルに等しければ、元のオブジェクトプログラムの処理にリターンする。一方、いずれかのブロックでチェックサムがオリジナルに不一致であった場合には、ステップＳ５に進み、ウイルスに感染したものと判断し、処理を中断する。

【００４７】図１２は本発明によるウイルス診断機構１８の第３実施例を示した機能ブロック図であり、この実施例はソースプログラムのレビジョン情報を利用するようにしたことを特徴とする。図１２において、第３実施例のウイルス診断機構はレビジョン情報検出部６８，レビジョン判断部７０およびオリジナル・レビジョン情報格納部７２で構成される。

【００４８】通常、オブジェクトプログラムはプログラムの先頭エリアにバージョンアップなどの改訂の様子を示すためレビジョン領域を設けている。このレビジョン領域には作成年月日，作成時刻，作成者名，プログラム名，バージョン番号などが格納されている。またオブジェクトプログラムは、ディスクユニットのディスク媒体上ではファイルとして扱われていることから、ディスク媒体上のファイル中にあるレビジョン領域も含む。

【００４９】そこで、ウイルス診断機構１８のオリジナル・レビジョン情報格納部７２にコンパイラで生成する際にオブジェクトプログラムの作成年月日（更新年月日を含む）７４，作成時刻（更新時刻を含む）７６，作成者名７８，プログラム名８０およびバージョン番号８２などをオリジナル・レビジョン情報としてセットしておく。

【００５０】このウイルス診断機構１８を埋め込んだオブジェクトプログラムの前段の処理が終わって起動入力を受けると、レビジョン情報検出部６８でソースプログラムのレビジョン領域から現在のレビジョン情報を検出してレビジョン判断部７０に引き渡す。レビジョン判断部７０は検出されたレビジョン情報とオリジナル・レビジョン情報格納部７２の格納情報とを比較し、一致すれば続行出力を生じ、不一致であればウイルスに感染したものとして中断出力を生ずる。

【００５１】レビジョン判断部７０における レビジョン情報の比較は、この実施例にあっては作成年月日７４，作成時刻７６，作成者名７８，プログラム名８０およびバージョン番号８２の全てについて行われ、いずれか１つでも不一致であるとウイルスに感染したものと判断して中断出力を行う。尚、ウイルス診断に使用するレビジョン情報としては、作成年月日，作成時刻，作成者名，プログラム名，バージョン番号のいずれか１つであってもよい。また、これ以外のレビジョン情報についても同様である。

【００５２】図１３は図１２のウイルス診断機構１８の第３実施例の処理動作を示している。まずステップＳ１でオブジェクトプログラムのレビジョン領域の情報を検出し，ステップＳ２で，予めセットしているオリジナルのレビジョン情報に一致するか否か判断し、一致すればリターンしてオブジェクトプログラムを続行し，不一致であればウイルスに感染したものとして、ステップＳ３で処理を中断する。

【００５３】図１４は本発明のウイルス診断機構１８の第４実施例を示したもので，この実施例はディスクアドレスを用いるようにしたことを特徴とする。第３実施例のウイルス診断機構１８はディスクアドレス検出部８４，ディスクアドレス比較部８６およびオリジナル・ディスクアドレス格納部８８で構成される。

【００５４】コンパイラにより作成されたオブジェクトプログラムは，ターゲットとなる計算機システムの入出力サブシステムを構築するディスクユニットに格納される。このため，オブジェクトプログラムには格納先を示すディスクアドレスとして例えばボリューム番号，ファイル番号およびトラックアドレスが記述されている。そこで，コンパイラでオブジェクトプログラムの中にウイルス診断機構１８を生成して埋め込む際に、オリジナル・ディスクアドレス格納部８８にソースプログラムの格納先となるディスクアドレスを示すボリューム番号９０，ファイル番号９２およびトラックアドレス９４などを格納しておく。この場合のアドレスは、開始アドレス，終了アドレスあるいはオブジェクトプログラムの一連のアドレスのいずれであってもよい。

【００５５】このウイルス診断機構１８を埋め込んだオブジェクトプログラムの実行でウイルス診断機構１８が起動入力を受けると、ディスクアドレス検出部８４でオブジェクトプログラムに現時点で記述されているディスクアドレス、例えばボリューム番号，ファイル番号およびトラックアドレスを検出してディスクアドレス比較部８６に引き渡す。

【００５６】ディスクアドレス比較部はオリジナル・ディスクアドレス格納部８８からオリジナルとしてのボリューム番号９０，ファイル番号９２およびトラックアドレス９４を読み出し、ディスクアドレス検出部８４からの検出情報と比較する。検出情報とオリジナル情報が一致すればウイルスに感染していないものと判断して、オブジェクトプログラムを続けて処理する続行出力を生ずる。検出情報とオリジナル情報が不一致であればウイルスによる感染でディスクアドレスの部分が破壊されたものと判断し、中断出力を生ずる。

【００５７】図１５は図１４のウイルス診断機構１８の第４実施例の処理動作を示している。まずステップＳ１でディスクアドレスを検出し、ステップＳ２でオリジナルアドレスとの一致，不一致を判断し，一致していれば通常処理にリターンし、不一致であればウイルスに感染

したものとして．ステップＳ３で処理を中断する。図１６は本発明によるウイルス診断機構１８の第５実施例を示した機能ブロック図であり、この第５実施例にあってはオブジェクトプログラム全体をオリジナルと比較してウイルス感染を判断するようにしたことを特徴とする。

【００５８】第５実施例のウイルス診断機構１８は実行オブジェクト読込部９６．オブジェクト比較部９８およびオリジナル・オブジェクト格納部１００で構成され、オリジナル・オブジェクト格納部１００にはオリジナルのオブジェクトプログラム１０２がそのまま格納されている。図１７は図１６に示した第５実施例のウイルス診断機構１８の生成の様子を示している。

【００５９】図１７において、コンパイラ１２に設けた診断オブジェクト生成部１４は、オブジェクトファイル２２０に対する１回目の出力でウイルス診断機構１８を埋め込んだオブジェクトプログラム１６を格納する。続いて診断オブジェクト生成部１４の機能により．ウイルス診断機構１８を埋め込んでいないオブジェクトプログラム１０２を２回目に出力してオブジェクトファイル装置２２０に格納する。

【００６０】ターゲットとなる計算機システム１０４に対しては、１回目に出力したウイルス診断機構１８を埋め込んだオブジェクトプログラム１６がイニシャルプログラムロード（ＩＰＬ）され、ＯＳまたはプログラムとして実行される。このＯＳまたはプログラムとしてのウイルス診断機構１８付きのオブジェクトプログラム１６の実行において．図１６に示したウイルス診断機構１８の処理が行われ．オリジナル・オブジェクト格納部１００の機能によりオブジェクトファイル装置２２０に２回目に出力されて格納されているオブジェクトプログラム１０２がオリジナルとして読み込まれて診断に使用される。

【００６１】図１８は図１６に示した第５実施例のウイルス診断機構１８の処理動作を示している。まずステップＳ１でメモリのワーク領域に現在実行しているオブジェクトプログラムを読み込んで展開する。続いてステップＳ２で外部のファイル装置２２０などに格納している計算機システム１０４では使っていないオリジナルのオブジェクトプログラム１０２を同じくワーク領域に読み込んで展開し．ステップＳ１で読み込んだ実行しているオブジェクトプログラムとの比較をコマンド単位に行う。ここでコマンド単位の比較は、変数については処理ごとに異なるから、比較対象から除外する。

【００６２】このようなコマンド単位の比較でオリジナルと全て一致すればウイルスに感染していないものと判断してオブジェクトプログラムの処理にリターンする。一方．コマンド単位の比較でオリジナルと不一致が生じた場合にはウイルスに感染したものと判断し、ステップＳ３で処理を中断する。尚．第５実施例のウイルス診断機構１８にあっては、図１７に示したようにオブジェクトプログラムのサイズが大きい場合にはプログラム全体の比較判断となるために診断処理に時間がかかることから．ウイルス診断機構１８の起動は計算機システム１０４のアイドルルーチンを検出して空き時間に行うことが望ましい。勿論．サイズの小さいオブジェクトプログラムであればオブジェクトのプログラムの実行ごとに行ってもよい。

【００６３】図１９は本発明によるウイルス診断機構１８の第６実施例を示した機能ブロック図である。この第６実施例はオブジェクトプログラム全体の比較判断を行うと同時に、比較判断に用いるオリジナル・オブジェクトプログラムを圧縮形式で出力し、比較判断の際に伸長して元のオブジェクトプログラムに復元することで行うようにしたことを特徴とする。

【００６４】この第６実施例のウイルス診断機構１８は実行オブジェクト読込部１０６，オブジェクト比較部１０８．圧縮オブジェクト格納部１１０および伸長部（復元部）１１４で構成される。圧縮オブジェクト格納部１１０には圧縮されたオブジェクトプログラム１１２が格納されている。図２０は図１９に示した第６実施例のウイルス診断機構１８を生成する様子を示している。

【００６５】コンパイラ１２に設けた診断オブジェクト生成部１４は．１回目の出力で図１９のウイルス診断機構１８を埋め込んだオブジェクトプログラム１６をオブジェクトファイル装置２２０に格納する。続いて２回目の出力でウイルス診断機構１８を埋め込んでいないオブジェクトプログラムを出力するが、この実施例にあっては診断オブジェクト生成部１４に圧縮アルゴリズムが設けられており．オブジェクトプログラムを圧縮した後に出力して、オブジェクトファイル装置２２０に圧縮オブジェクトプログラム１１２として格納する。

【００６６】診断オブジェクトプログラム生成部１４による圧縮アルゴリズムとしては、例えば２進算術符号化アルゴリズムが使用され．オブジェクトプログラム１６のサイズを元の２％程度まで圧縮することができる。従って．圧縮オブジェクトプログラム１１２の格納領域を大幅に低減することができる。オブジェクトファイル装置２２０に格納されたウイルス診断機構１８が埋め込まれたオブジェクトプログラム１６は．ターゲットとなる計算機システム１０４にイニシャルプログラムロード（ＩＰＬ）されてＯＳまたはプログラムとして実行される。

【００６７】この計算機システム１０４におけるオブジェクトプログラム１６の実行において．ウイルス診断機構１８が起動するとオブジェクトファイル２２０に格納されている圧縮オブジェクトプログラム１１２を読み出し．伸長部１１４で伸長した後に、オブジェクト比較部１０８で、現在実行しているオブジェクトプログラムとの比較判断を行う。

【００６８】圧縮オブジェクトプログラム１１２を伸長

する身長部１１４はウイルス診断機構１８専用ではなく、計算機システム１０４がもっている伸長プログラムを利用して行うことが望ましい。図２１は図１９に示したウイルス診断機構１８の第５実施例の処理動作を示す。

【００６９】まずステップＳ１で圧縮オブジェクトプログラムを読み込み、ステップＳ２で圧縮オブジェクトプログラムを伸長して元のオリジナル・オブジェクトプログラムに展開する。このような圧縮オブジェクトプログラムの読込みと元のオブジェクトプログラムへの伸長は、計算機システム１０４におけるメモリのワーク領域上で行われる。

【００７０】続いてステップＳ３で、現在実行中のオブジェクトプログラムを同じくワーク領域に読み込む。続いてステップＳ４で、圧縮形式から復元したオリジナル・オブジェクトプログラムと実行オブジェクトプログラムを例えばコマンド単位に比較して、一致の有無を判断する。この場合も第５実施例と同様、コマンドに含まれる変数は判断対象から除外する。２つのオブジェクトプログラムが一致していればウイルスによる感染はないものとして、元のオブジェクトプログラムの処理にリターンする。

【００７１】一方、コマンド単位の比較で不一致が起きた場合にはウイルスによる感染と判断し、ステップＳ５に進んで処理を中断する。この第６実施例にあっても、オブジェクトプログラム全体の比較判断になることから、プログラムサイズが大きい場合にはウイルス診断処理に時間がかかるので、計算機システム１０４のアイドル状態で診断処理を行うことが望ましい。勿論、プログラムサイズが小さければ、オブジェクトプログラムの中でウイルス診断処理を行えばよい。

【００７２】更に本発明の他の実施例として、以上説明した第１実施例から第６実施例のウイルス診断機構１８に加え、図３に示したコンパイラ部１２でオブジェクトプログラム１６を出力する際に、オブジェクトプログラム１６に更新不可属性をセットして出力させることが望ましい。即ち、オブジェクトプログラム１６がウイルスに感染すると、図８，図９に示したように感染によりオブジェクトプログラムの書替えが行われる。このようなウイルス感染による書替えを禁止するため、コンパイラから出力する際に更新不可属性をセットしてオブジェクトプログラム１６を出力しておく。このような更新不可属性のセットはオブジェクトプログラム１６にウイルス感染を防ぐワクチンを注入した機能をもつ。

【００７３】即ち、本発明によりオブジェクトプログラムの中にウイルス診断機構を埋め込むと同時に、必要ならば更新不可属性のセットなどのワクチンを設けておくこともウイルス感染による被害を防ぐためには望ましい。但し、更新不可属性のようなワクチンは特定のウイルスには利くが別のウイルスには効果がない場合が多く、予防的な意味で設けることになる。

【００７４】

【発明の効果】以上説明してきたように本発明によれば、ウイルスの感染がオブジェクトプログラムに埋め込まれたウイルス診断機構により判り、しかも感染が判ると処理を中断することから、ウイルス感染による被害を最小限に抑え、適切なウイルスの感染防止対策をとることができる。

【００７５】また、オブジェクトプログラムに対するウイルス診断機構の埋込みはコンパイラに設けた診断オブジェクト生成機能によりコンパイラ段階で自動的に行われる。このため、ソースプログラムの製造段階でウイルス診断機構を意識する必要がなく、ソースプログラムの製造行程に負担を与えない。

【００７６】また全てのソースプログラムのコンパイルについてオブジェクトプログラムの中にウイルス診断機構が自動的に埋め込まれ、これによってターゲット計算機のＯＳやプログラムがウイルスに感染したことを早期に発見して、且つ被害の拡大を確実に防止できる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明で用いるコンパイラのハードウェア構成図

【図３】本発明によるウイルス診断機構の生成を示した説明図

【図４】コンパイラの機能構成を示した説明図

【図５】本発明のウイルス診断機構の第１実施例を示したブロック図

【図６】図５の処理動作を示したフローチャート

【図７】ウイルス感染処理の一例を示したフローチャート

【図８】ウイルス感染前と感染後のプログラム構造を示した説明図

【図９】図５のウイルス診断機構によりウイルス感染が判断された場合のプログラム構造の説明図

【図１０】本発明のウイルス診断機構の第２実施例を示したブロック図

【図１１】図１０の処理動作を示したフローチャート

【図１２】本発明のウイルス診断機構の第３実施例を示したブロック図

【図１３】図１２の処理動作を示したフローチャート

【図１４】本発明のウイルス診断機構の第４実施例を示したブロック図

【図１５】図１４の処理動作を示したフローチャート

【図１６】本発明のウイルス診断機構の第５実施例を示したブロック図

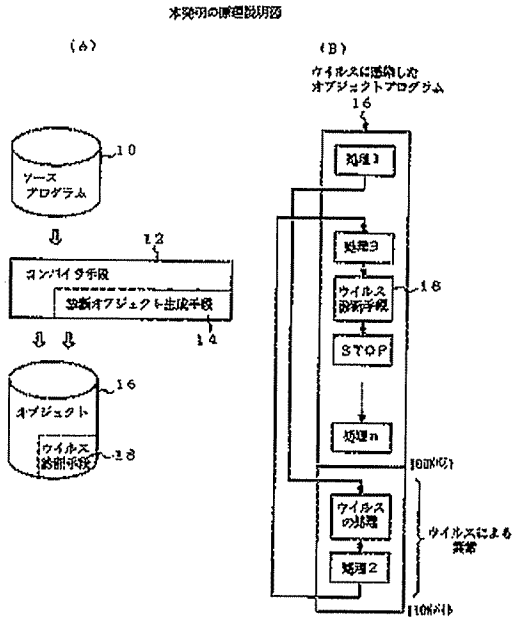
【図１７】図１６のウイルス診断機構の生成と診断処理の説明図

【図１８】図１６の処理動作を示したフローチャート

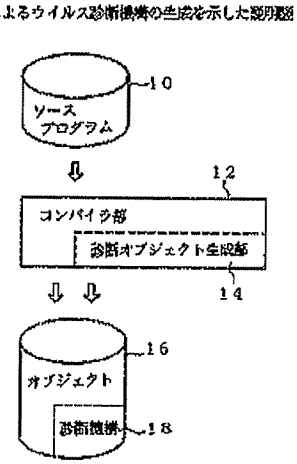
【図１９】本発明のウイルス診断機構の第６実施例を示

したブロック図
【図２０】図１９のウイルス診断機構の生成と診断処理の説明図
【図２１】図１９の処理動作を示したフローチャート
１０：ソースプログラム
１２：コンパイラ部
１４：診断オブジェクト生成部
１６：オブジェクトプログラム
１８：ウイルス診断機構
２０：プログラムサイズ検出部
２２：サイズ判断部
２４：オリジナルサイズ格納部
２６：語彙解析処理部
２８、３２，３６，４２：中間ファイル
３０：構文解析処理部
３８：コード最適化部
４４：コード生成部
４８：感染前のオブジェクトプログラム
５２：感染後のオブジェクトプログラム
５０－１～５０－ｎ：処理ブロック
５４：ウイルスの処理ブロック
５６：感染後の本発明のオブジェクトプログラム
６０：感染による増加領域
６２：チェックサム検出部
＊６４：チェックサム判断部
６６：オリジナルチェックサム格納部
６８：レビジョン情報検出部
７０：レビジョン判断部
７２：オリジナル・レビジョン情報格納部
８４：ディスクアドレス検出部
８６：ディスクアドレス比較部
８８：オリジナル・ディスクアドレス格納部
９６、１０６：実行オブジェクト読込部
９８、１０８：オブジェクト比較部
１００：オリジナル・オブジェクト格納部
１０４：計算機システム
１１０：圧縮オブジェクト格納部
１１２：圧縮オブジェクトプログラム
１１４：伸長部（復元部）
２００：主記憶装置
２０２：主記憶制御装置
２０４：ＣＰＵ
２０６：チャネル装置
２１０：デバイスバス
２２０，２３０、２５０、２６０：ファイル装置
２４０：中間ファイル
２７０：シンボルテーブル
＊

【図１】

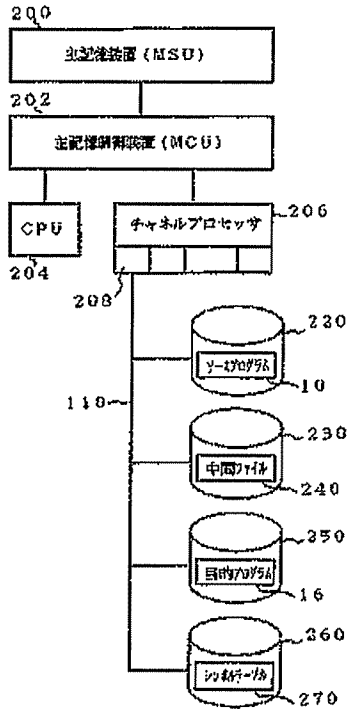


【図３】



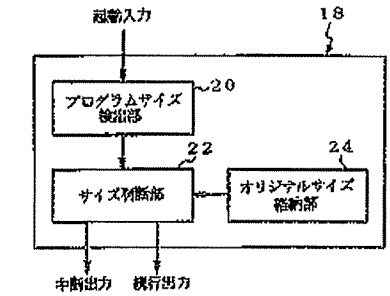
【図２】

本発明で用いるコンパイラのハードウェア構成図



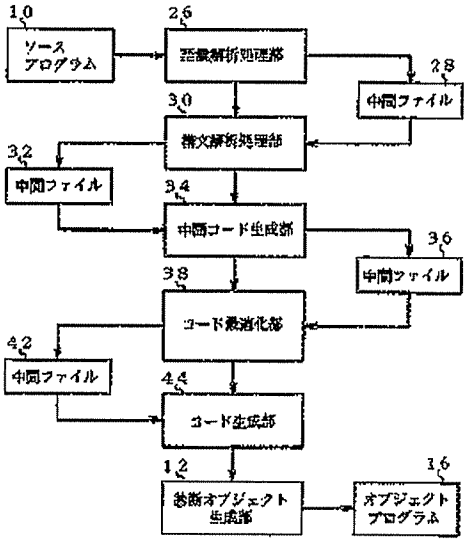
【図５】

本発明のウイルス診断機構の第１実施例を示したブロック図



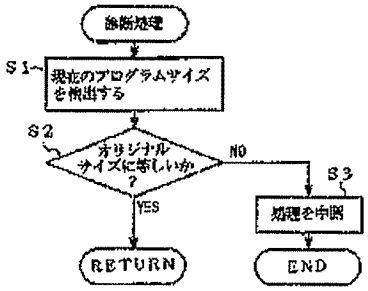
【図４】

コンパイラの機能構成を示した説明図



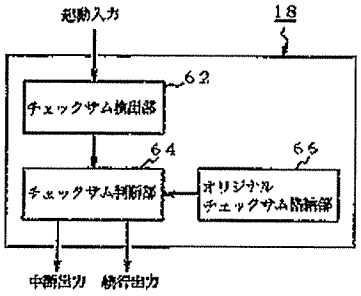
【図６】

図５の処理動作を示したフローチャート



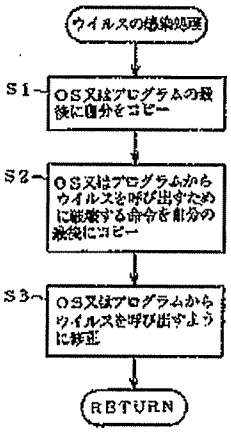
【図１０】

本発明のウイルス診断機構の第２実施例を示したブロック図



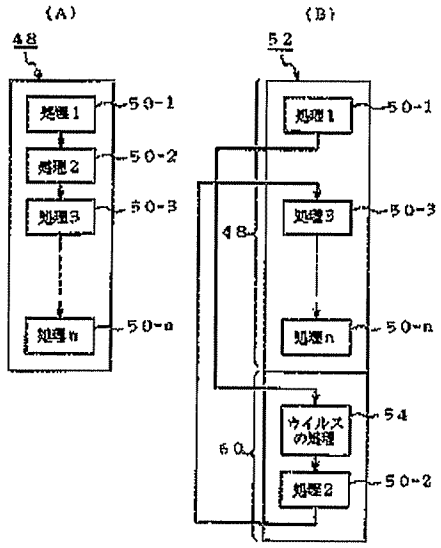
【図７】

ウイルス感染処理の一例を示したフローチャート



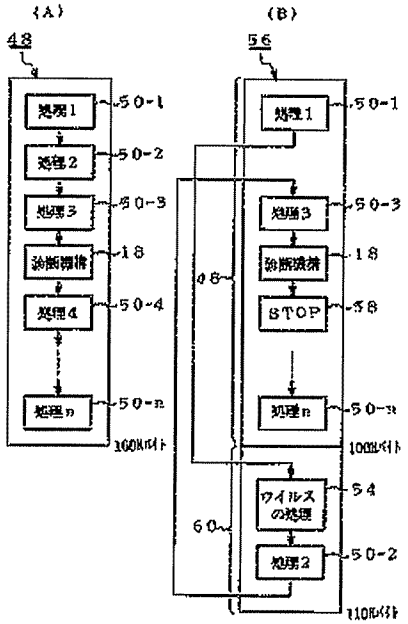
【図８】

ウイルス感染前と感染後のプログラム構造を示した説明図



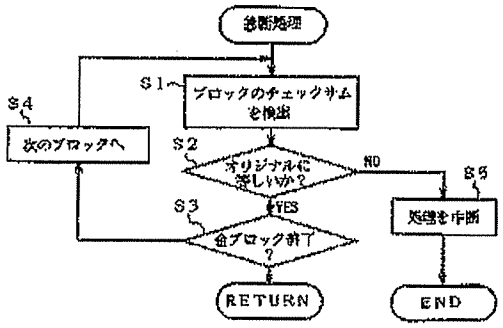
【図９】

図５のウイルス診断機構によりウイルス感染が判断された場合のプログラム構造の説明図



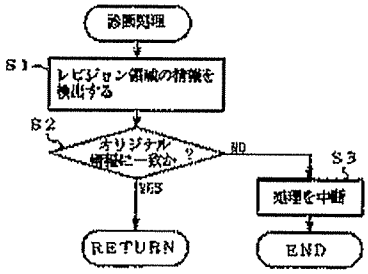
【図１１】

図１０の処理動作を示したフローチャート



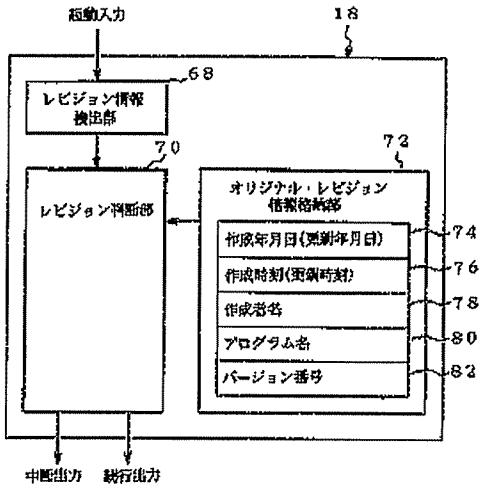
【図１３】

図１２の処理動作を示したフローチャート



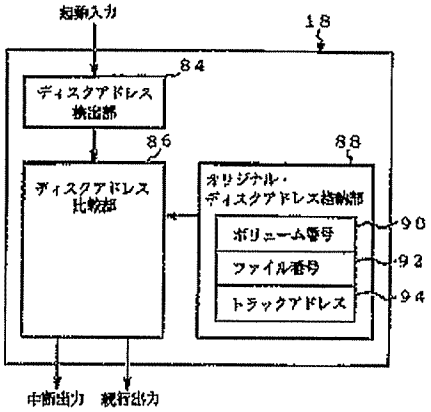
【図１２】

本発明のウイルス診断機構の第３実施例を示したブロック図



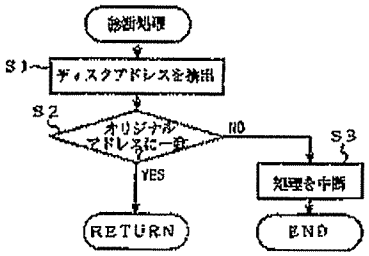
【図１４】

本発明のウイルス診断機構の第４実施例を示したブロック図



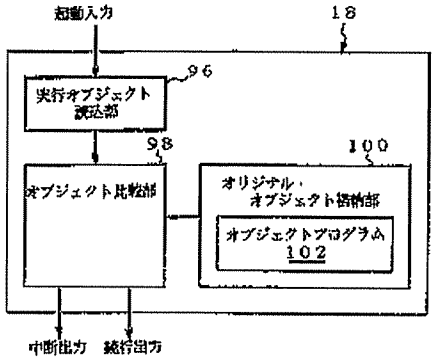
【図１５】

図１４の処理動作を示したフローチャート



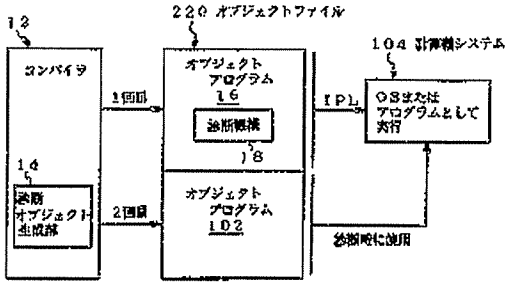
【図１６】

本発明のウイルス診断機構の第５実施例を示したブロック図



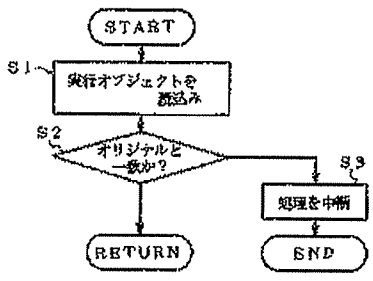
【図１７】

図１６のウイルス診断機構の生成と診断処理の説明図



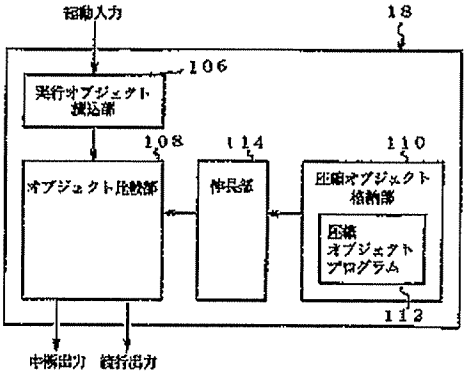
【図１８】

図１６の処理動作を示したフローチャート



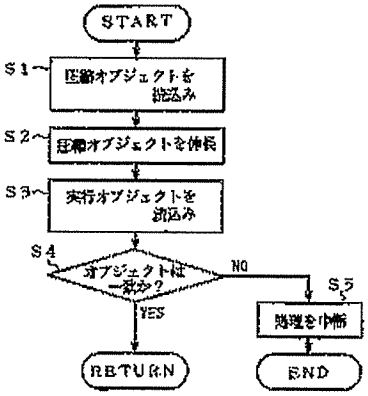
【図１９】

本発明のウイルス診断機構の第６実施例を示したブロック図



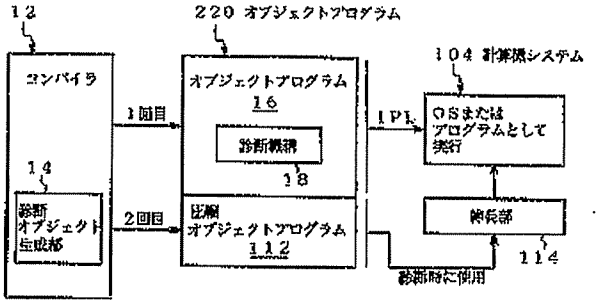
【図２１】

図１９の処理動作を示したフローチャート



【図２０】

図１９のウイルス診断機構の生成と診断処理の説明図



フロントページの続き

(51)Int.Cl.°		識別記号	庁内整理番号	F I	技術表示箇所
G06F	9/445				
	9/45				
	11/34		A	9290－5B	